UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trad mark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
09/226,577	01/07/99	CHANEY J	SAM1.0058

WM31/1024

SHERMAN & SHERMAN
2029 CENTURY PARK EAST
SEVENTEENTH FLOOR
LOS ANGELES CA 90067

EXAMINER	
NEWTON, G	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 10/24/01

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trad marks

Offic Action Summary	Application No.	Applicant(s)	
	09/226,577	CHANEY, JACK	
	Examiner	Art Unit	
	Gregory A Newton	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondenc address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 October 1999* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claim 1 is rejected under 35 U.S.C. **102(b)** as being anticipated by **Muratani et al** (US 6,061,451).

Claim 1 recites a method of copy protecting a digital signal representing audio visual information. However, the limitations of claim 1 are found to read on patented invention by **Muratani et al**. APPARATUS AND METHOD FOR RECEIVING AND DECRYPTING ENCRYPTED DATA AND PROTECTING DECRYPTED DATA FROM ILLEGAL USE. For disclosure of protection of audio visual data, see e.g. ABSTRACT.

For disclosure of encoded data, e.g. MPEG protocol, see ABSTRACT. For conversion of the signal into a copy protected signal utilizing a data signal representing copy protection data, reference is made to page 14 of the application specification. The data after copy protection is described on page 14 as not usable by any devices, and so it is understood to be an encryption function, and the copy protection data is understood to be keying data. Henceforth, the copy protection function will be referred to as the first

encryption function, and the copy protection data will be referred to as keying data. Reference is also made to page 15 of the specification where disclosures of utilizing an XOR function for encryption and decryption with the keying data, which is a well known encryption technique. Other functions besides the XOR are also available for encryption with keying data.

For disclosure of another scrambling function subsequent to the first above listed function, see figure 3 of Muratani, where the second scramble circuit is illustrated. This second scrambling function will henceforth be described in this office action as the second encryption function.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 2-32 are rejected under 35 U.S.C. **103(a)** as being unpatentable over **Muratani et al** (US 6,061,451) in view of **Menezes**, HANDBOOK OF APPLIED CRYPTOGRAPHY.

Claim 2 recites the method of claim 1 with further limitations. **Muratani** is silent with respect to disclosures of transmitting the encrypted signal with keying data to a

receiver in the exact fashion as limitations recited in claims, although different possible embodiments are suggested to one of ordinary skill in the art. Therefore, reference is made to the **Menezes** reference of note, HANDBOOK OF APPLIED CRYPTOGRAPHY. For teachings of using two encryption functions, see page 234. For illustration of sending keying data with information (audio visual) data, see page 16, figure 1.7, and caption describing key exchange channel. The encryption function E depicted in figure 1.7 would be embodied as the double encryption method as taught on page 234. The Muratani device is an embodiment of Menezes teachings of double encryption in section 7.2.3 concerning multiple encryption methods.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to combine the teachings of Muratani with the teachings of Menezes in order to perform double encryption of audio visual data. One of ordinary skill in the art would have been motivated to do this in order to thwart attempts at retrieving an open signal at the set-top box, as disclosed in Muratani, column 3, last paragraph, and top of column 3.

Claims 3 and 4 recite the method of claims 1 and 3 respectively, with further limitations. For sending all data as a single signal, see page 13, figure 1.6, where there is shown one unsecured channel for all data, including keying data. For combining the keying data with a signal, it is well known that in order to encrypt the data, it must be combined with the data in an encrypting fashion. See also Muratani, column 3, last paragraph for disclosure of keying data being transmitted with other data.

Claim 5 recites the method of claim 3 with further limitations. For illustration of receiving the single signal in a receiver, see e.g. **Muratani**, figure 3, where three receptions occur.

For disclosure of removing keying data from received data single signal, see figure 1.6 of **Menezes**. It would have been obvious to one of ordinary skill in the art to store the keying data, perhaps in a buffer, to synchronize computer instructions. For receiving keying data with other data combined, refer to figure 1.6 of Menezes, where one unsecured channel is illustrated.

For teachings of recovery and decryption of the second encryption function, refer to Menezes figure 1.6, where the decryption function is illustrated. The decryption function illustrated in figure 1.6 is understood with respect to claim 5 to be a double encryption decryptor function as taught in section 7.2.3 of Menezes concerning multiple encryptions.

Reconverting the regained copy protected signal back into said encoded signal using an inverse copy protection function by using said stored copy protection data is understood to be decryption by the second (inverse) encryption function using the keying data, as taught in Menezes, section 7.2.3, concerning multiple encryption.

Decoding the encoded signal to recover the digital signal is found illustrated in Muratani, figure 1, item 16.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to combine the teachings of Muratani with the teachings of Menezes in order to decrypt the doubly encrypted data. One of ordinary

skill in the art would have been motivated to do this because an inverse decryption phase must be obtained to retrieve the audio visual signals.

Claim 6 recites a method with limitations in common with the claim 5 limitations, but without the step of storing the keying data. This claim therefore is rejected in view of the same prior art of record and in accordance with the same rationale of applying the inverse function, i.e. decryption.

Claim 7 recites a method of recovering an audiovisual signal from a doubly encrypted digital signal. For illustration of extracting of a keying data signal from the signal, refer to **Menezes** figure 1.7.

It would have been obvious for one of ordinary skill in the art to store keying data, perhaps in a buffer, in order to synchronize computer instructions.

As for extracting and descrambling the signal to recover the copy protected signal, this is understood to be decryption of the signal by the inverse of the second encryption function, leaving the signal which is still encrypted by the first encryption function.

Reconverting the copy protected signal into an encoded signal using an inverse copy protection function using copy protection data is understood to be decryption of the signal with the inverse of the first encryption function using the keying data.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to combine the teachings **Menezes** with the teachings of **Muratani** in order to decrypt audio visual information. One of ordinary skill in the art would have been motivated to do this to thwart attempts to derive an open signal from

the set top box as discussed in Muratani, column 3, last paragraph, and top of column 4.

Claims 8-14 are system claims corresponding to the method claims 1-7, and are rejected in view of the same prior art of record and in accordance with the same rationale.

Claim 15 recites a system for recovering an audio visual signal from a digital signal including a scrambled signal and a copy protection data signal representing copy protection data. However, the limitations in claim 15 are found to read on patent reference of note by **Muratani**. The scrambling and copy protection functions are understood to be two encryption functions as illustrated in figure 3, and the copy protection data are understood to be keying data, e.g. as disclosed in column 2, lines 45-50.

For illustration of a receiver and descrambler module connected via a link, see figure 3, i.e. security module item 70. For a communication interface for communicating with a receiver via a link, see figure 1, where receiver item 12 connects via a link with interface item 26.

For illustration of a descrambler for descrambling an incoming scrambled signal from the receiver via the link, see figure 1, item 22.

For illustration of a receiver with a second communication interface for communicating with the descrambler module via the link, see figure 2, the two interfaces for security module item 70.

A reconverter for converting an incoming copy protected signal from the descrambler back into said audiovisual signal using an inverse copy protection function wherein the inverse function utilizes stored copy protection data is understood to refer to limitations of the inverse of the first cryptographic function which uses the keying data for decryption. It is obvious that one of ordinary skill in the art would want to store the keying data, perhaps in a buffer, in order to synchronize computer instructions.

Muratani et al are silent with respect to explicit disclosure of removing keying data from the signal and storing it in a memory device, extracting the scrambled signal from the digital signal, although the descramblers are illustrated e.g. in figure 3.

However, reference is made to Menezes' figures 1.6 and 1.7, where keying data is transmitted over single and multiple channels. One of ordinary skill in the art would have wanted to store the keying data, perhaps in a buffer, in order to synchronize computer instructions. Menezes and Muratani et al both teach double encryption, and Muratani et al use double encryption in order to make secure the signal leading to the set top decryptor/descrambler, although not in the same exact order as the Muratani et al device.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to combine the teachings of **Muratani et al** with the teachings of **Menezes** in order to arrange a double encryption configuration to protect a signal to a set top descrambler/decryption device. One of ordinary skill in the art would have been motivated to do this by the disclosures within Muratani et al, e.g. bottom of column 2 and top of column 3, which are discussions related to motivations to protect

the set top signal from getting siphoned from an open signal between the module and the receiver.

Claim 16 recites the system of claim 15 with further limitations of the incoming audiovisual signal into the receiver is encoded and scrambled, and wherein the receiver further includes a decoder for decoding said reconverted signal.

Muratani et al disclose a device where the incoming audio visual signal is doubly encrypted in order to secure the signal going to and from a set top descrambler/decryptor as illustrated e.g. in figure 3. For disclosures of the signal being encoded, see e.g. ABSTRACT of Muratani et al.

Claims 17 and 18 recite the system of claim 15 with further limitations of the descrambler module comprising a PCMIA card, and the first and second communication interfaces being IS679 compatible interfaces. **Muratani et al** and **Menezes** are silent with respect to explicit disclosure of outfitting such a double encryption device with such hardware. However, one of ordinary skill in the art would have wanted to implement such hardware into the Menezes teachings and Muratani et al illustrations of their double encryption device in order to enable the device. One of ordinary skill in the art at the time of the invention would have been motivated to do this because the devices are commercially available.

Claim 19 recites the system of claim 15 with further limitations of the link being one or more communication mediums configured for carrying audiovisual signals. The device of **Muratani et al** is configured with links for transmitting audiovisual signals, as

is disclosed e.g. in the ABSTRACT, in order to protect the signals to and from the set top box.

Claim 20 recites a method of protecting signals transmitting between a scrambling module and a receiver. Copy protection is found on page 14 of the specification to render the signal unusable, implying that it is encryption method. The **Muratani et al** device is conceived to protect a signal transmitting between the set top descrambler module and the receiver, as depicted e.g. in figure 3.

For illustration of receiving an audiovisual digital signal in a receiver, see Muratani et al, e.g. ABSTRACT, or figures 2 and 3.

For disclosure of generating copy protection data representing copy protection data, see e.g. Muratani el al column 5, section titled First Embodiment, paragraph 4. Where copy protection data is understood to be equivalent to keying data.

For illustration of transmitting a digital signal from the receiver to the descrambler module via a link, see e.g. figures 2 and 3.

For illustration of descrambling the scrambled audiovisual signal in the module to obtain an audiovisual signal, see figure 2.

Converting the audiovisual signal in the descrambler module into a copy protected signal using a copy protection function is understood as an encryption of the signal within the module by one of the encryption functions, which are disclosed e.g. column 5, lines 45-50, or illustrated in figure 3.

Transmission of the encrypted signal from the module to the receiver via a link is illustrated e.g. in figures 2 and 3. Reconversion of the copy protected signal to the

audiovisual using inverse copy protection function by using the data signal is understood to be decryption utilizing the keying data, as disclosed in Muratani et al e.g. column 5, lines 20-50.

Muratani et al are silent with respect to explicit disclosure of the exact protocol of the above steps, i.e., descrambling the received signal within the set top module with one descrambling function, and subsequently reencrypting the signal for the transmission from the set top module to the receiver, where it is again decrypted. However, protection of the signal between the set top module and the set is the main concern of the Muratani et al device, as is disclosed in the ABSTRACT. Furthermore, Muratani el al suggest other embodiments to ones with ordinary skill in the art, e.g. at the top of column 5. Further still, examiner takes official notice that encryption between devices configured together are common and well known in the art, e.g. encryption between a pc and a disc storage device in order to secure data transmission therebetween.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to combine the teachings of **Muratani et al** with a decryptor within the set top module, and subsequently re-encrypting the signal for the transmission from the set top module to the receiver in order to provide a secure signal between the set top module and the receiver. One of ordinary skill in the art would have been motivated to do this because such a technique of encryption between devices in a configuration is well known in the art.

Claim 21 recites the method of claim 20 with further limitations of generating the copy protection data signal in the receiver. This is understood to be equivalent to generating key data in the receiver, and is disclosed in Muratani et al, e.g. column 5, lines 30-35.

Claim 22 recites the method of claim 21 with further limitations. **Muratani** et al are silent with respect to explicit disclosure of transmitting keying data via a link. For illustration of transmitting keying data signal via a link, see **Menezes**, figure 1.7. At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to combine the teachings of **Muratani et al** with the teachings of **Menezes** in order to provide a secure signal between a set top module and a receiver. One of ordinary skill in the art would have been motivated to do this by considering the enablement concerns of the Muratani device which are left to one of ordinary skill in the art, i.e., enabling the scrambling functions disclosed by Muratani.

Claim 23 recites the method of claim 20 with further limitations. For disclosure of the audiovisual signal being encoded and scrambled, refer e.g. to ABSTRACT of Muratani et al reference of note.

Claim 24 recites the method of claim 23 with further limitations of decoding the audiovisual receiver after the step of reconverting. For disclosure of decoding in the receiver following reconversion (decrypting), refer to Muratani et al e.g. figures 1 and 2.

Claim 25 recites the method of claim 20 with further limitations of the module being a PCMIA card. For disclosure of utilization of an IC card within the **Muritani et al** device, refer to e.g. column 6, line 6. Muratani et al are silent with respect to explicit

disclosure of the card being a PCMIA card. However, one of ordinary skill in the art at the time the invention was made would have been motivated to enable the Muratani et al device with a PCMIA card because of its commercial availability.

Claim 26 recites the method of claim 20 with further limitations. For disclosure of communication mediums configured for carrying audiovisual signals, refer to **Muratani et al**, e.g. column 2, lines 25-30.

Claim 27 recites the method of claim 20 with further limitations. For disclosure of link interface devices, refer to **Muratani et al**, e.g. column 2, line 31. Muritani et al are silent with respect to explicit disclosure of utilization of an IS679 compatible interface for the link. However, one of ordinary skill in the art at the time the invention was made would have been motivated to implement a certain interface for the link between the module and the receiver, as depicted in figures 1-3 of Muratani et al. One would have been motivated to employ a specific device because of its commercial availability for specific enablements of the Muratani et al device.

Claims 28-32 recite copy protection system claims corresponding to the signal recovery system claims 15-19, and are rejected in view of the same prior art of record and in accordance with the same rationale.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Gregory A Newton whose telephone number is 703-305-1373. The examiner can normally be reached on 9-6 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert DeCady can be reached on 703-305-9595. The fax phone numbers for the organization where this application or proceeding is assigned are 703-746-7239 for regular communications and 703-746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

gn

gn
October 15, 2001

PHUNG M. CHUNG
PRIMARY EXAMINER